AMENDMENT AFTER FINAL OFFICE ACTION
EXPEDITED PROCEDURE
GROUP ART UNIT 2764
Docket No. 1083.1048/MS

Serial No. 09/000,924
Page 8

REMARKS

In the Office Action mailed March 14, 2000 the Examiner rejected claims 1-5, 9, 12, 15, and 18-21 under 35 USC 103 as being unpatentable over Hasebe (US Patent No. 5,392,351 - Hasebe #1) in view of Hasebe (US Patent No. 5,761,651 - Hasebe #2) and further in view of Iwayama (US Patent No. 5,832,083) and further asserted that claims 1-21 are rejected. As a preliminary matter, the Examiner has referred to Patent No. '083 as being issued to Hasebe et al. While Hasebe is listed as an inventor on the '083 Patent, the Applicants presume the Examiner intended to refer to Iwayama et al. wherever Patent No. '083 is referenced in the Office Action. The Applicant respectfully request clarification. Further, although it is unclear from the Office Action under what rationale claims 6-8, 10, 11, 13, 14, 16, 17 were rejected, the foregoing claims 6-8, 10, 11, 13, 14, 16, 17 patentably distinguish over the references relied upon for rejecting claims 1-5, 9, 12, 15 and 18-21 as discussed herein below. Moreover, rejections of claims 6-8, 10, 11, 13, 14, 16, 17 are traversed. The Applicants respectfully request clarification regarding the rationale the Examiner rejects claims 6-8, 10, 11, 13, 14, 16, 17.

The foregoing rejections are respectfully traversed.

In the Office Action mailed March 14, 2000 the Examiner noted that claims 1-21 were pending, and rejected claims 1-21. Claims 1-13, 15, and 18-20 have been amended, new claim 22 has been added and, thus, in view of the forgoing claims 1-22 remain pending for reconsideration which is requested.

No new matter has been added in this Amendment.

SPECIFICATION

The specification has been amended to correct minor typographical errors.

AMENDMENT AFTER FINAL OFFICE ACTION
EXPEDITED PROCEDURE
GROUP ART UNIT 2764
Docket No. 1083.1048/MS

Serial No. 09/000,924
Page 9

CLAIM REJECTIONS

Present Invention

In the present invention a data protection system protects input data requiring authorization for use against unauthorized use of the input data during utilization of the input data. Therefore, the data protection system according to the present invention prevents unauthorized uses of the input data during utilization of the input data by determining whether the input data being utilized/processed (e.g., for example, as incorporated in data being created/prepared/generated by a user) requires authorization for use. Therefore, in the present invention "prepared data is prepared by a user, whereas "input data" is input from the database so as to be used for preparing the aforementioned "prepared data." If the input data being utilized/processed requires authorization for use, the system generates and appends link information in the prepared data (i.e., for example, data incorporating the input data requiring authorization for use) specifying the input data requiring authorization for use.

Hasebe #1

Hasebe #1 discloses a data protection system for preventing unauthorized copying of electronic data, such as computer software (Hasebe #1 at abstract, Col. 1, lines 6 - 9). The protected software is provided to the user encrypted on a storage medium such as an optical disk (Col. 1, lines 63 - 65; Col. 2, lines 27 - 29). The electronic key for decrypting the data is stored on the storage medium in encrypted form (Col. 1, line 66 - Col. 2, line 3). The vendor computer supplies encrypted permission information, for decrypting the encrypted electronic data, to the user computer via transmission or to the user in a document (Col. 2, lines 14 - 26). Upon decryption, the unencrypted software is available for execution by the user (Col. 3, lines 37 - 39; Col. 5, line 66 - Col. 6, line 2).

Hasebe #2

Hasebe #2 discloses a system for charging for use of digitized data such as software and for granting permission to use the data (Hasebe #2 at abstract; Col. 1, lines 7 - 9). The supplied data is decrypted for use by a software managing module (Col. 3, lines 46 - 65). Deciphering for subsequent use by the user is permitted only if an available credit balance exists in a charging table (Col. 4, lines 18 - 21). The available balance is subtracted based on the deciphering processing amount or the processing period of time for the ciphered software data (Col. 4, lines 23 - 25). The user can add to the remaining balance total to permit additional use of the data (Col. 4, lines 25 - 29).

Iwayama

Iwayama et al. discloses a system for authorized accessing of encoded electronic data such as computer software (Iwayama et al. at abstract; Col. 2, lines 11 - 15). The data is first stored as encoded data on a storage medium such as a compact disk (Col. 2, lines 30 - 33). The desired portion of encoded data will be decoded when a user inputs the identification information for the preferred data content (Col. 2, lines 61 - 65). When the decoding is completed, the system compares the decoded content identification information with the user-supplied content information (Col. 3, lines 14 - 19). If the two sets of information match, the system will output the selected data portion to the user (Col. 3, lines 19 - 22).

Combination of Hasebe#1, #2 and Iwayama

Combination of Hasebe #1, #2 and Iwayama would be a system incorporating the three systems disclosed in the forgoing references to grant permission for use of electronic data or software. However, the foregoing references, either alone or in combination, do not disclose or suggest preventing during utilization of input data that requires authorization for use certain

utilization/processing of the input data (e.g., storage, cut and paste) unless authorization is obtained.

Claim Recitations of the Present Invention

In contrast to the foregoing references, the present invention (as recited in amended claims 1, 12 and new claim 22, using the recitation of claim 1 as an example) comprises "means for preparing data embedding the input data", "means for generating information specifying the input data embedded in the prepared data", "means for appending the generated information to the prepared data", "means for utilizing the prepared data with the appended generated information by displaying the prepared data and the embedded input data" and "means for preventing storage of the embedded input data in a storage means to prevent unauthorized use of the embedded input data if the embedded input data is judged to require authorization for use." Further, in contrast to the foregoing references, the present invention (as recited in each of independent claims 4, 9, 18, 19, as amended, using the recitation of claim 4 as an example) comprises "means for preventing storage of the input data in a storage means during processing of the data when said input data has been judged to require authorization for use." For example, a benefit of these patentably distinguishing features is that the system judges if the input data utilized/processed (e.g., incorporated/embedded) in the prepared data requires authorization for use and the system prevents certain utilization/processing (e.g., storage, cut and paste, display) to be performed on the input data requiring authorization for use unless authorization is obtained. Further, for example, in the present invention storage of original input data requiring authorization and embedded in data created by a user may be forbidden by the system upon subsequent utilization of the created data to prevent unauthorized use of the embedded input data.

Further, in contrast to the foregoing references, the present invention (as recited in each of independent claims 4, 9, 15, 20 and 21 using the recitation of claims 4 as an example)

AMENDMENT AFTER FINAL OFFICE ACTION
EXPEDITED PROCEDURE
GROUP ART UNIT 2764
Docket No. 1083.1048/MS

Serial No. 09/000,924
Page 12

comprises "storage means for storing process information indicating what kind of processing has been applied by said processing means." A benefit of this patentably distinguishing feature is that input data as processed by a user or the process information itself can be subsequently distributed as input data requiring authorization for use, thereby continuing the protection of the original input data.

Dependent claims 2-3, (depending, either directly or indirectly, from claim 1), 5-8 (depending either directly or indirectly from claim 4), 10-11 (depending either directly or indirectly from claim 9), 13-14 (depending, either directly or indirectly from claim 12), and 16-17 (depending, either directly or indirectly from claim 15) recite patentably distinguishing features of their own and further are also patentably distinguishing over the foregoing references at least due to their dependencies from independent amended claims 1, 4, 9, 12, and 15.

For example, claim 2 recites "means for preventing the cut and paste function with respect to the embedded input data to prevent unauthorized use of the embedded input data when the embedded input data requires authorization for use." This patentably distinguishing feature has the benefit of blocking cut and paste operations on the embedded input data requiring authorization for use.

Dependent claims 3 and 5 (using the recitation of claim 3 as an example) recite "means for determining whether the embedded input data requires authorization for use when the embedded input data is encrypted." A benefit of this patentably distinguishing feature is to determine if the embedded encrypted input data requires authorization for use, so that even though embedded input data is encrypted, the system still determines if the embedded input data requires authorization for use.

 Claim 6 depending from claim 4 recites that "the process information is differential data indicating a difference between the input data and the input data after having been processed."

Serial No. 09/000,924   Docket No. 1083.1048/MS
Page 13

Claim 10 depending from claim 9 recites "means for distributing the process information from said center as input data requiring authorization for use." Claim 11 depending from claim 9 recites "means for distributing data prepared by adding the process information to the input data to be processed from said center as input data requiring authorization for use."

Withdrawal of the rejection of claims 1-21, and allowance of claims 1-21 and new claim 22 is respectfully requested.

Entry of this Amendment is respectfully requested because the foregoing amendments and remarks clarify the patentably distinguishing features of the present invention over the foregoing references.

Serial No. 09/000,924
Page 14

Conclusion

In light of the amendments and remarks presented above, Applicant submits that this Application is now in condition for allowance, and such action is hereby respectfully requested.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,

STAAS & HALSEY LLP

By _____

Mehdi Sheikerz
Registration No. 41,307

Date _Jun e 14 , 2000_
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500